

Before the  
Federal Communications Commission  
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

Comments in Support of Petitions for Reconsideration

These comments illustrate the following points:

1. Google's decision to combine its users' personally-identifiable information with the vast browsing data of its advertising subsidiary, DoubleClick, which accesses consumer data on 75.3% of all websites that use an ad server — a decision Google made *after* the submission of edge-provider data on which the FCC relied — renders the FCC's finding inaccurate with respect to the percentage of web information Google can access.
2. The FCC's findings regarding encryption failed to consider consumers' use of encrypted virtual private networks (VPNs) that are available at low cost and even for *free*. At a minimum, the FCC must explain why it's necessary to impose unique privacy rules on ISPs when a solution is already widely-available in the marketplace at little or no cost.
3. The FCC's failure to consider the fact that its factual findings regarding edge providers directly contradict the factual findings made by the FTC — the federal agency who is the nation's expert on edge provider regulation — constitutes arbitrary agency action as a matter of law.
4. The FCC's failure to consider arguments regarding the impact of its rules on competition among ISPs and edge providers in the online advertising and big data markets constitutes arbitrary agency action as a matter of law.
5. Privacy is a personal right, and it's reasonable for consumers to assume the law will protect their person from one network to another — but the FCC's rules do not provide such protection.

6. There is no legal barrier whatsoever to the FCC treating section 222 of the Communications Act as if it were coextensive with the FTC's approach to privacy.

### The FCC's factual findings are not supported by substantial evidence

The FCC's factual findings in the BIAS privacy order do not accurately reflect how information about consumers is collected, aggregated, and monetized on the internet.

*First*, the FCC's findings are inaccurate regarding the percentage of websites to which Google has access. The FCC relied on an ex parte presentation made on June 17, 2016, to support the agency's finding that Google does not "have access to more than approximately 25 percent of web pages."<sup>1</sup> This ex parte presentation did not consider Google's ability to use DoubleClick data.<sup>2</sup> At the time this ex parte presentation was prepared, Google had *chosen* to limit its access to that percentage of webpages based on a pledge it made to get its acquisition of DoubleClick approved.<sup>3</sup> But Google had the *capability* to access more than 25 percent of web pages, *and it quietly decided to exercise that capability on June 28, 2016, only 1 day after the FCC's official comment period expired*.<sup>4</sup> According to a complaint filed by Consumer Watchdog and Privacy Rights Clearinghouse at the Federal Trade Commission, Google began combining its users' personally-identifiable information with the vast browsing data of its advertising subsidiary, DoubleClick. With this change, Google can—

now track users' activity on its Android mobile phones, with an 88% market share of smartphones worldwide, and from any website that uses Google Analytics, hosts YouTube videos, or displays ads served by DoubleClick or AdSense. In other words, Google has given itself the power to track users across the overwhelming majority

---

<sup>1</sup> BIAS Privacy Order at para. 30 (citing Dillon Reisman and Arvind Narayanan, Princeton Center for Information Technology Policy, WC Docket No. 16-106, Ex Parte Presentation at 32 (filed June 17, 2016), available at <https://ecfs-api.fcc.gov/file/60002354966.pdf>).

<sup>2</sup> See id. (treating DoubleClick as separate from Google in its analysis of Google's 3rd-party presence on websites). The FCC also excluded [google-analytics.com](http://google-analytics.com) for reasons the agency did not explain.

<sup>3</sup> See Complaint, Request for Investigation, Injunction, and Other Relief Submitted by Consumer Watchdog and Privacy Rights Clearing House to the Federal Trade Commission on December 16, 2016, at p. 1, available at [http://www.consumerwatchdog.org/resources/ftc\\_google\\_complaint\\_12-5-2016docx.pdf](http://www.consumerwatchdog.org/resources/ftc_google_complaint_12-5-2016docx.pdf).

<sup>4</sup> See id.

of websites in use in the world today, many of which appear to users to be entirely unconnected from Google.<sup>5</sup>

According to Datanyze, Google's DoubleClick access consumer data on 75.3% of all websites that use an ad server,<sup>6</sup> including Google.com and YouTube, which alone account for 53.3 billion monthly visits.<sup>7</sup> To put these numbers into perspective, when DoubleClick partnered with 800 local newspapers and 200 TV stations to create a private ad exchange in February, 2014, the consortium touted the "vast size and scale of [its] collective audience ... with a total of 240 million monthly visitors"<sup>8</sup> — which amounts to less than 1/2 of a percent of the 53.3 billion monthly visits to Google.com and YouTube. Google's decision to use its DoubleClick data—a decision it made only after the FCC's information on the topic had already been filed, render inaccurate the FCC's finding that Google only sees consumer information from about 25% of web pages. Based on its Android and DoubleClick market shares, Google sees more consumer information on the web than any ISP.

*Second*, the FCC's findings regarding encryption failed to consider consumers' use of encrypted virtual private networks (VPNs). The FCC focused its encryption analysis entirely on the encryption of traffic by edge providers.<sup>9</sup> Services like "Private Internet Access" ([privateinternetaccess.com](http://privateinternetaccess.com)) offer encrypted VPN service for up to 5 devices with unlimited bandwidth for \$6.95 a month, and others like Spotflux and Tor offer free VPN services.<sup>10</sup> These services do not rely on an edge provider's decision with respect to encryption. A VPN encrypts all traffic and even permits a consumer to "change your geographic location by overriding the IP address assigned by your ISP with one drawn from [the VPNs] pool of servers."<sup>11</sup> With a VPN service, a consumer's data remains

---

<sup>5</sup> Id. at pp. 2-3.

<sup>6</sup> See Datanyze ad service market share data for ad servers at <https://www.datanyze.com/market-share/ad-servers/>.

<sup>7</sup> See SimilarTech at <https://www.similartech.com/technologies/doubleclick>.

<sup>8</sup> See Garrett Sloane, Google, Local News Sites Create Private Exchange, Adweek (Feb. 24, 2014), available at <http://www.adweek.com/digital/google-local-news-sites-create-private-exchange-155918/>.

<sup>9</sup> See BIAS Privacy Order at para. 34.

<sup>10</sup> Private Internet Access VPN, PC Mat, available at <http://www.pcmag.com/article2/0,2817,2414799,00.asp>.

<sup>11</sup> Id.

hidden while in transit over an ISP's network even while using an open Wi-Fi network (but not to the edge provider or web page the consumer visits).<sup>12</sup> Yet the FCC did not even consider the fact that consumers can hide their traffic from their ISPs using low-cost or *free* encryption services. The FCC's failure to consider the availability and use of VPNs was a fatal error that renders "arbitrary and capricious" its decision in the BIAS privacy order.<sup>13</sup> *At a minimum, the FCC must explain why it's necessary to impose unique privacy rules on ISPs when a free solution is already widely-available in the marketplace.*

*Third*, the FCC failed to address the Federal Trade Commission's finding, raised in Tech Knowledge's reply comments<sup>14</sup> (among others), that ISPs "are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like [internet access providers], operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles."<sup>15</sup> This factual finding from the federal agency who is the nation's expert on edge providers directly contradicts the FCC's own factual finding, yet the FCC did not mention it. "[A]n agency's refusal to consider evidence bearing on the issue before it constitutes arbitrary agency action ...."<sup>16</sup>

### The rules insulate edge providers from competition

The FCC's BIAS privacy order is also arbitrary and capricious because it failed to consider the impact of its rules on competition among ISPs and edge providers in the online advertising and big data markets. As Tech Knowledge has stated before:

---

<sup>12</sup> Id.

<sup>13</sup> See, e.g., *State Farm*, 463 U.S. at 43, 103 S.Ct. 2856; *Comcast Corp. v. FCC*, 579 F.3d 1, 8 (D.C.Cir.2009).

<sup>14</sup> See Tech Knowledge Reply Comments at p. 4 (July 6, 2016), available at <http://techknowledge.center/wp-content/uploads/2016/07/TK-filing-privacy-reply-07-06-16-Filed.pdf>.

<sup>15</sup> Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at p. 56 (2012), available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

<sup>16</sup> See *State Farm*, 463 U.S. at 43, 103 S.Ct. 2856; *Comcast Corp. v. FCC*, 579 F.3d 1, 8 (D.C.Cir.2009).

Private consumer information is like any other secret. Even if you only tell a few friends you think you can trust, your secret will likely spread. And the Internet companies the FCC refuses to hold accountable for your privacy — like Google — aren't your friends. They're in the business of selling your secrets — secrets so valuable that Google is now the largest company the world has ever known. Yet the FCC plans to exempt Google and the Internet's other biggest secret-sellers from its new privacy rules. It's the equivalent of adopting a nuclear weapons ban that applies to everyone except the United States and Russia — the world's biggest nuclear powers — and claiming the ban will keep the world safe from nuclear attack.<sup>17</sup>

Tech Knowledge's reply comments noted that the imposition of discriminatory rules on ISPs would harm competition by muzzling ISPs while permitting edge providers to continue collecting and using consumer information,<sup>18</sup> yet the FCC ignored the issue. "[A]n agency's 'failure to respond meaningfully' to objections raised by a party renders its decision arbitrary and capricious."<sup>19</sup> Here, *the FCC did not respond at all.*

### **The rules expose consumers to irrational gaps in privacy protection**

In the context of consumer privacy, the FCC's decision to define "broadband internet access service" in the same way it's defined in the "net neutrality context" is irrational. It might have been reasonable to exempt certain types of networks, like Wi-Fi networks in coffee shops, from net neutrality rules, because such networks present no potential for competitive harm to edge providers. But that rationale does not apply to the FCC's decision to exempt those same networks from its privacy rules. A consumer who uses a Wi-Fi network at the coffee shop should have the same expectation of privacy as the consumer sitting next to them who is using an LTE connection. Their interest in protecting their privacy does not change with their change in connectivity.

When privacy applies to all companies alike, like the FTC's privacy framework, consumers can readily understand to the extent to which their information is protected. It's unlikely, however, that the average consumer will understand the subtle nuances in the FCC's definition of BIAS. In

---

<sup>17</sup> See Tech Knowledge Statement On FCC Privacy Announcement (Mar. 10, 2016), available at <http://techknowledge.center/blog/2016/03/tech-knowledge-statement-on-fcc-privacy-announcement/>.

<sup>18</sup> See Tech Knowledge Reply Comments at p. 10.

<sup>19</sup> BNSF Ry. Co. v. Surface Transp. Bd., 741 F.3d 163, 168 (D.C. Cir. 2014), quoting PSEG Energy Resources & Trade LLC v. FERC, 665 F.3d 203, 208 (D.C. Cir. 2011).

the coffee shop example above, it's unreasonable to assume the consumer who is using Wi-Fi understands that the FCC's rules do not protect them, but do protect the LTE user sitting beside them.

*Privacy is a personal right, and it's reasonable for consumers to assume the law will protect their person from one network to another.* For this reason alone, privacy protections must be harmonized across all internet companies.

### Reconsidering the current rules won't leave consumers unprotected

The notion that consumers will be left unprotected if the FCC's harmonizes its approach with the FTC's privacy framework is absurd. *There is no legal barrier whatsoever to the FCC treating section 222 of the Communications Act as if it were coextensive with the FTC's approach to privacy.* To the extent the express language of section 222 is inconsistent with the FTC approach, the FCC can simply forbear from that language as it has done with other provisions in Title II. And to the extent section 222 would not otherwise apply to an action the FTC prohibits, the FCC can use its Title I authority to fill in the gap. This is neither complicated nor controversial.

Respectfully submitted,

TECH KNOWLEDGE

By: \_\_\_\_\_ /s/ FBCJR

Fred B. Campbell, Jr.  
Director  
14925 Doe Ridge Road  
Haymarket, VA 20169  
703-470-4145

March 6, 2017

